

*Petition for Inter Partes Review
of U.S. Patent No. 9,413,721*

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

Sophos Ltd. and Sophos Inc.,
Petitioners

v.

Webroot Inc.,
Patent Owner.

Case No. IPR2023-00491

U.S. Patent No. 9,413,721

Petition for *Inter Partes* Review of U.S. Patent No. 9,413,721

Mail Stop **PATENT BOARD**
Patent Trial and Appeal Board
U.S. Patent and Trademark Office
P.O. Box 1450
Alexandria, VA 22313-1450

TABLE OF CONTENTS

	<u>Page</u>
I. INTRODUCTION	1
II. MANDATORY NOTICES	2
A. Real Parties-in-Interest 37 C.F.R. § 42.8(b)(1).....	2
B. Related Matters Under 37 C.F.R. § 42.8(b)(2)	2
1. Current Litigation.....	2
2. Administrative Proceedings	2
C. Lead and Backup Counsel.....	2
D. Service of Information Under 37 C.F.R. § 42.8(b)(4)	4
III. PAYMENT OF FEES	4
IV. REQUIREMENTS OF <i>INTER PARTES</i> REVIEW	4
A. Standing.....	4
B. Identification of Challenge and Relief Requested	5
C. How the Challenged Claims Are to Be Construed Under 37 C.F.R. § 42.104(b)(3).....	7
D. How the Challenged Claims Are Unpatentable Under 37 C.F.R. § 42.104(b)(4).....	8
E. Supporting Evidence Under 37 C.F.R. § 42.104(b)(5)	8
V. THRESHOLD REQUIREMENT FOR <i>INTER PARTES</i> REVIEW	9
VI. LEVEL OF SKILL IN THE ART	9
VII. STATE OF THE ART	10
VIII. OVERVIEW OF THE '721 PATENT	14
IX. DETAILED CHALLENGE	20
A. Ground 1: Claims 1, 8, 9, 14, and 15 are obvious under § 103 over Liu, Tuvell, and Kester.....	20

TABLE OF CONTENTS
(continued)

	<u>Page</u>
1. Prior Art Overview.....	20
2. Motivation to Combine and Reasonable Expectation of Success	22
3. Analysis.....	25
X. PTAB DISCRETION SHOULD NOT PRECLUDE INSTITUTION.....	62
A. PTAB should not exercise its discretion to deny institution under <i>Fintiv</i>	62
1. Factor 1: Whether Institution Will Increase the Likelihood of a Stay in the District Court.....	63
2. Factor 2: District Court Schedule	64
3. Factor 3: Petitioners’ Investment in the IPR Outweighs Forced Investment in Litigation to Date	67
4. Factor 4: The Petition Raises Unique Issues	68
5. Factor 5: Institution Will Provide the Board an Opportunity to Invalidate Claims That Could Be Later Reasserted against Others	69
6. Factor 6: Other Circumstances Support Institution	69
B. PTAB should not exercise its discretion to deny institution under <i>Becton</i> and <i>Advanced Bionics</i>	70
XI. CONCLUSION.....	71
XII. CERTIFICATE OF WORD COUNT	72

TABLE OF AUTHORITIES

	<u>Page(s)</u>
Cases	
<i>10X Genomics, Inc. v. Bio-Rad Labs., Inc.</i> , IPR2020-00086, Paper 8 (PTAB Apr. 27, 2020)	7
<i>Advanced Bionics LLC v. MED-EL Elektromedizinische Gerate GmbH</i> , IPR2019-01469, Paper 6 (PTAB Feb. 13, 2020)	70
<i>Apple Inc. v. Fintiv, Inc.</i> , IPR 2020-00019, Paper 15 (May 13, 2020).....	64, 69
<i>Apple v. Seven Networks</i> , IPR2020-00255, Paper 13 (July 28, 2020)	67
<i>Becton, Dickinson & Co. v. B. Braun Melsungen AG</i> , IPR2017-01586, Paper 8 (Dec. 15, 2017)	70
<i>Cizion, LLC v. Kerr Machine Co.</i> , PGR2020-00065, Paper 10 (Dec. 3, 2020)	65
<i>HTC Corp. v. Cellular Communications Equip., LLC</i> , 877 F.3d 1361 (Fed. Cir. 2017)	7
<i>Micron Tech., Inc. v. Godo Kaisha IP Bridge 1</i> , IPR2020-01008, Paper 10 (Dec. 7, 2020)	65
<i>Mylan Pharm. Inc. v. Sanofi-Aventis Deutschland GMBH</i> , IPR2018-01680, Paper 22, 17 (Apr. 3, 2019)	65
<i>Nidec Motor Corp. v. Zhongshan Broad Ocean Motor Co.</i> , 868 F.3d 1013 (Fed. Cir. 2017)	8
<i>Oticon Medical AB v. Cochlear Ltd.</i> , IPR2019-00975 Paper 15 (Oct. 16, 2019)	70

TABLE OF AUTHORITIES

(continued)

	<u>Page(s)</u>
<i>Samsung Elec. 's Co., Ltd. et al v. Staton Techniya, LLC</i> , IPR2022-00302, Paper 13, 10 (July 11, 2022)	67
<i>Sand Revolution II, LLC v. Continental Intermodal Grp.</i> , IPR2019-01393, Paper 24 (June 16, 2020).....	63, 68
<i>Sotera Wireless, Inc. v. Masimo Corp.</i> , IPR2020-01019, Paper 12 (Dec. 1, 2020)	63
<i>Vivid Techs., Inc. v. Am. Sci. & Eng'g, Inc.</i> , 200 F.3d 795 (Fed. Cir. 1999)	8
<i>VMware Inc. v. Intellectual Ventures II LLC</i> , IPR2020-00859, Paper 13 (Nov. 5, 2020)	64
<i>Volkswagen Grp. of Am., Inc. v. Arigna Tech. Ltd.</i> , IPR2021-01321, Paper 10 at 7 (Feb. 15, 2022).....	64
<i>Webroot, Inc. v. AO Kaspersky Lab</i> , No. 6:22-cv-00243-ADA-DTG (W.D. Tex.).....	66
<i>Webroot, Inc. v. Forcepoint LLC</i> , No. 6:22-cv-00342-ADA-DTG (W.D. Tex.).....	2, 69
<i>Webroot, Inc. v. Sophos Ltd.</i> , No. 6:22-cv-00240-ADA-DTG (W.D. Tex.).....	2
<i>Western Digital Corp. v. Kuster</i> , IPR2020-01391, Paper 10 (Feb. 16, 2021).....	63
<i>Western Digital Corp. v. SPEX Techs., Inc.</i> , IPR2018-00082, Paper 11 (Apr. 25, 2018).....	7

TABLE OF AUTHORITIES
(continued)

	<u>Page(s)</u>
Other Authorities	
MPEP § 2143(I)(G).....	49
CHRIS McNAB, <i>Network Security Assessment</i> (2d Ed.) 161 (2008)	15
<i>PTAB Consolidated Trial Practice Guide</i> 59 (Nov. 2019).....	69

*Petition for Inter Partes Review
of U.S. Patent No. 9,413,721*

TABLE OF EXHIBITS

Exhibit Number	Document
1001	U.S. Patent No. 9,413,721 (“the ’721 Patent”)
1002	File History of the ’721 Patent
1003	Declaration of Dr. Richard Newman
1004	Curriculum Vitae of Dr. Richard Newman
1005	U.S. Patent Pub. No. 2006/0075504 to Liu (“Liu”)
1006	U.S. Patent Pub. No. 2008/0086773 to Tuvell (“Tuvell”)
1007	U.S. Patent Pub. No. 2005/0223001 to Kester (“Kester”)
1008	U.S. Patent No. 7,392,543 to Szor (“Szor”)
1009	U.S. Patent Pub. No. 2007/0016953 to Morris (“’953 Publication”)
1010	U.S. Patent No. 7,966,650 to Manring (“Manring”)
1011	Stipulation Waiving IPR Claims in District Court Litigation
1012	Excerpt from Transcript of Motions Hearing in <i>Webroot, Inc., et al. v. AO Kaspersky Lab</i> , No. 6:22-cv-00243-ADA-DTG (W.D. Tex.) (Dec. 9, 2022)
1013	Excerpt from HENRY F. KORTH AND ABRAHAM SILBERSCHATZ, DATABASE SYSTEM CONCEPTS, McGraw-Hill, New York, 2006.
1014	K. J. Biba, “Integrity Considerations for Secure Computer Systems,” MTR-3153, The MITRE Corporation (Apr. 1977).

*Petition for Inter Partes Review
of U.S. Patent No. 9,164,800*

TABLE OF EXHIBITS
(continued)

Exhibit Number	Document
1015	David E. Bell and Leonard J. LaPadula, “Secure Computer Systems: Mathematical Foundations,” MTR-2547, The MITRE Corporation (Mar. 1973).

I. INTRODUCTION

Sophos Ltd. and Sophos Inc. petition for *inter partes* review (IPR), seeking cancellation of claims 1, 8, 9, 14, and 15 of U.S. Patent No. 9,413,721 (“the ’721 Patent,” EX-1001). This petition demonstrates that there is at least a reasonable likelihood that Petitioners will prevail on at least one challenged claim based upon prior-art references that the USPTO did not have before it during prosecution.

The ’721 Patent describes and claims a distributed architecture that examines objects (like computer programs) to determine if they are malware. The patent describes sending information about an object to a first server, and if the object has not been seen before, requesting additional information about the object. The first server then sends this information to a central server, which in turn distributes information about the object to other servers. The patent further describes storing information about the objects in databases associated with each server, and tracking how many times an object has been seen.

None of this was new. As demonstrated below, distributed architectures that meet all of the limitations of the challenged claims were commonplace. Each supposed innovation of the ’721 Patent existed before the ’721 Patent was published: Malware-detection systems already used network-based distributed client

computers, coupled with a server that interrogated suspect objects and processed data about those objects (including counting the number of times the object had been seen), and then storing that data in databases. Claims 1, 8, 9, 14, and 15, therefore, should be cancelled as unpatentable under 35 U.S.C. § 103.

II. MANDATORY NOTICES

A. Real Parties-in-Interest 37 C.F.R. § 42.8(b)(1)

Sophos Ltd., and Sophos Inc. are the real parties-in-interest.

B. Related Matters Under 37 C.F.R. § 42.8(b)(2)

1. Current Litigation

The '721 Patent is the subject of two pending litigations in a suit brought by Patent Owner against Sophos Ltd. and one other defendant. *Webroot, Inc. v. Sophos Ltd.*, No. 6:22-cv-00240-ADA-DTG (W.D. Tex.), Dkt. No. 1 (the “District Court Action”), and *Webroot, Inc. v. Forcepoint LLC*, No. 6:22-cv-00342-ADA-DTG (W.D. Tex.), Dkt. No. 1. These cases are now consolidated, along with three others, as *Webroot, Inc. v. AO Kaspersky Lab*, No. 6:22-cv-00243-ADA-DTG (W.D. Tex.).

2. Administrative Proceedings

There are no other administrative proceedings at issue.

C. Lead and Backup Counsel

Petitioners designate the following counsel:

*Petition for Inter Partes Review
of U.S. Patent No. 9,413,721*

Lead Counsel	Backup Counsel
Ryan Iwahashi (Reg. No. 63,378) Gibson, Dunn & Crutcher LLP 1881 Page Mill Road Palo Alto, CA 94304-1211 Tel: (650) 849-5367 RIwahashi@gibsondunn.com	Josh Krevitt (<i>pro hac vice</i> motion requested) Gibson, Dunn & Crutcher LLP 1881 Page Mill Road Palo Alto, CA 94304-1211 Tel: (212) 351-2490 JKrevitt@gibsondunn.com
	Brian A. Rosenthal (<i>pro hac vice</i> motion requested) Gibson, Dunn & Crutcher LLP 200 Park Avenue New York, NY 10166-0193 Tel: (212) 351-2339 BRosenthal@gibsondunn.com
	Timothy P. Best (<i>pro hac vice</i> motion requested) Gibson, Dunn & Crutcher LLP 333 South Grand Avenue Los Angeles, California 90071-1504 Tel: (213) 229-7659 TBest@gibsondunn.com

Petitioners respectfully request authorization to file motions for Josh Krevitt, Brian Rosenthal, and Timothy Best to appear before the USPTO *pro hac vice*. Mr. Krevitt, Mr. Rosenthal, and Mr. Best are experienced litigating attorneys and are currently serving as lead counsel for Petitioners in the District Court Action. Each has established familiarity with the subject matter of this proceeding. Petitioners

intend to file a motion to appear *pro hac vice* under 37 C.F.R. § 42.10. Pursuant to 37 C.F.R. § 42.10(b), powers of attorney accompany this petition.

D. Service of Information Under 37 C.F.R. § 42.8(b)(4)

Service of any documents via hand delivery may be made at the mailing address of lead and backup counsel designated above. Petitioners also hereby consent to electronic service, and service via electronic mail may be made at the email addresses provided above for the lead and backup counsel.

III. PAYMENT OF FEES

Pursuant to 37 C.F.R. §§ 42.103 and 42.15(a), the required fee is being submitted herewith. The Office is authorized to charge any fee deficiency, or credit overpayment, to Deposit Account 50-1408. Any additional fees due in connection with this petition may be charged to the foregoing account.

IV. REQUIREMENTS OF INTER PARTES REVIEW

A. Standing

Pursuant to 37 C.F.R. § 42.104(a), Petitioners certify that the '721 Patent is available for IPR and that Petitioners are not barred or estopped from requesting IPR of the claims on the grounds identified herein. Specifically, Petitioners certify the following: Petitioners have not filed a civil action challenging the validity of the

*Petition for Inter Partes Review
of U.S. Patent No. 9,413,721*

'721 Patent; this petition is filed not more than one year from March 11, 2022, the date on which the Sophos Ltd. received service of the complaint alleging infringement of the '721 Patent; the estoppel provisions of 35 U.S.C. § 315(e)(1) do not prohibit this *inter partes* review; and this petition is filed after the later of (a) the date that is nine months after the date of the grant of the '721 Patent or (b) the termination of any post-grant review of the '721 Patent.

B. Identification of Challenge and Relief Requested

Pursuant to 37 C.F.R. § 42.104(b), Petitioners request that the Board institute IPR of claims 1, 8, 9, 14, and 15 (the “Challenged Claims”) of the '721 Patent on one or more grounds under 35 U.S.C. § 103.¹ The precise relief that Petitioners request is that claims 1, 8, 9, 14, and 15 be cancelled in view of the following prior art references:

Reference	Qualifying Date	Prior Art Under
Liu	April 6, 2006	§102(b)
Tuvell	April 10, 2008	§102(b)
Kester	October 6, 2005	§102(b)

¹ The application that issued as the '721 Patent was filed before March 16, 2013, and thus is subject to the pre-AIA versions of 35 U.S.C. §§ 102 and 103, and thus all references to Sections 102 and 103 refer to their pre-AIA versions.

*Petition for Inter Partes Review
of U.S. Patent No. 9,413,721*

The '721 Patent is a U.S. patent resulting from Application No. 13/372,375, which was filed on February 13, 2012. The application claims priority to provisional application No. 61,443,095, which was filed on February 15, 2011. Thus, based on the face of the '721 Patent, Petitioners believe that the Challenged Claims are entitled to a priority date no earlier than February 13, 2012.

In the related district court litigation, Patent Owner has asserted that the claims were conceived earlier than the date of the provisional application. Since Petitioner's prior art references qualify as prior art under § 102(b) regardless, Patent Owner's assertions have no impact upon the analysis. In any case, for just the purpose of this IPR petition, Petitioners do not dispute Patent Owner's contention that the claims were conceived earlier than the date of the provisional application.

Each of the references cited above is prior art. Liu was published on April 6, 2006, and thus is prior art at least under §102(b). Tuvell was published on April 10, 2008 and is prior art under §102(b). Kester was published on Oct. 6, 2005, and is prior art under §102(b). None of these prior art references was cited during the prosecution of the application that issued as the '721 Patent. *See, e.g.*, Ex-1001 at 1 (listing references cited). The Challenged Claims are unpatentable based on the following:

*Petition for Inter Partes Review
of U.S. Patent No. 9,413,721*

Ground	Claims	Basis for Rejection
1	1, 8, 9, 14, and 15	§103 by Liu in view of Tuvell and Kester

C. How the Challenged Claims Are to Be Construed Under 37 C.F.R. § 42.104(b)(3)

Petitioners do not believe any constructions have an impact on the invalidity analyses set forth herein. *See HTC Corp. v. Cellular Communications Equip., LLC*, 877 F.3d 1361, 1367–68 (Fed. Cir. 2017) (affirming the Board’s application, absent an express construction of a term). Although Petitioners and Patent Owner disagree over the construction of certain terms in the parallel District Court litigation, for the purpose of this Petition, Petitioners rely on Patent Owner’s proposed constructions (plain and ordinary meaning). *See 10X Genomics, Inc. v. Bio-Rad Labs., Inc.*, IPR2020-00086, Paper 8 at 17–22 (PTAB Apr. 27, 2020) (instituting IPR and clarifying that a Petitioner need only identify “[h]ow the challenged claim is to be construed” for purposes of the petition and that “judicial efficiency will be enhanced by allowing Petitioner to rely upon a claim construction that Patent Owner is relying upon in the related district court litigation to assert infringement of the challenged patent”); *see also Western Digital Corp. v. SPEX Techs., Inc.*, IPR2018-00082, Paper 11 at 12 (PTAB Apr. 25, 2018) (“Petitioner’s statement that its Petition ‘is

based on the claim constructions urged by Patent Owner’ in related District Court litigation . . . suffices to identify claim constructions Petitioner is adopting for purposes of the requested review in compliance with § 104(b)(3).”).

Moreover, the Board “need only construe terms ‘that are in controversy, and only to the extent necessary to resolve the controversy.’” *Nidec Motor Corp. v. Zhongshan Broad Ocean Motor Co.*, 868 F.3d 1013, 1017 (Fed. Cir. 2017) (quoting *Vivid Techs., Inc. v. Am. Sci. & Eng’g, Inc.*, 200 F.3d 795, 803 (Fed. Cir. 1999)). Because Petitioners base this Petition on constructions *Patent Owner* has advocated, the Petition does not present any controversy over claim meaning and the Board need not construe any terms. *Nidec*, 868 F.3d at 1017.

D. How the Challenged Claims Are Unpatentable Under 37 C.F.R. § 42.104(b)(4)

An explanation of how the Challenged Claims are unpatentable, including the identification of where each element of the claim is found in the prior art patents or printed publications, is provided below.

E. Supporting Evidence Under 37 C.F.R. § 42.104(b)(5)

The exhibit numbers of the supporting evidence relied upon and the relevance of the evidence to the Challenged Claims, including an identification of specific portions of the evidence that support the challenge, are provided below. A List of

Exhibits identifying the exhibits is also included in this petition pursuant to 37 C.F.R. § 42.63(e). The technical information and grounds for rejection explained in the petition are further supported by the Expert Declaration of Dr. Richard Newman, attached as Exhibit 1003.

V. THRESHOLD REQUIREMENT FOR *INTER PARTES* REVIEW

Under 35 U.S.C. § 314(a), institution of *inter partes* review requires “a reasonable likelihood that the petitioners would prevail with respect to at least one of the claims challenged in the petition.” This Petition meets this threshold for each ground.

VI. LEVEL OF SKILL IN THE ART

A person of ordinary skill in the art (“POSITA”) in February 2012 would have had at least a Bachelor’s degree in Computer Science, Computer Engineering, Electrical Engineering, or an equivalent discipline, and at least two years’ worth of experience developing computer networking or network architecture, or a Master’s degree in a related field. EX-1003 ¶17. Alternately, a POSITA could have four or more years of work experience in computer networking and in the development of client-server systems. *Id.*

VII. STATE OF THE ART

The '721 Patent expressly incorporates by reference (but does not claim priority to) U.S. Patent Publication No. 2007/0016953 (the "'953 Publication"), published Jan. 18, 2007. EX-1001, 2:15-19. The '953 Publication shares one common inventor with the '721 Patent, and claims priority to a foreign application that was filed on June 30, 2005. EX-1009. The '953 Publication thus describes the state of the art as it existed in 2005—nearly six years before the '721 Patent's provisional application was filed.

Signatures: The '953 Publication describes how the art used signatures to determine if a file potentially contained malware: "A typical anti-malware product, such as anti-virus scanning software, scans objects or the results of an algorithm applied to the object or part thereof to look for *signatures in the object that are known to be indicative of the presence of a virus*. Generally, the method of dealing with malware is that when new types of malware are released, for example via the Internet, these are eventually detected. Once new items of malware have been detected, then the service providers in the field generate signatures that attempt to deal with these and these signatures are then released as updates to their anti-malware programs." EX-1009, [0003] (emphasis added).

With respect to other prior-art references, the '953 Publication also states that: “[i]n the case of these prior art systems, the request for authorisation to run the file that is sent by a local computer to the central computer may comprise sending a checksum or ‘signature’ or ‘key’ that uniquely represents the file.” EX-1009, [0007]. Thus, the '953 Publication describes using signatures to uniquely identify files or portions of files to servers.

Databases: The '953 Publication also describes how the art used databases containing the categorization of known files to determine if a potential file is safe: “WO-A-2004/097602 describes a system that analyses computer files received or generated by a local computer and compares these with a database of known files to determine whether a particular file is known and if so whether it has been known about long enough that it can be regarded as ‘safe’.” *Id.*, [0005].

“Community-Based” Systems: The '953 Publication also describes how networked anti-malware systems existed in the art. *Id.*, [0007]. In a networked anti-malware system, local computers sent information about unknown files to a central computer; if the central computer had seen the file before, the central computer could deem the file safe or malicious, and if the central computer had not seen the file before, the entire file could be sent to the central computer for analysis:

U.S. Pat. No. 6,944,772, U.S. Pat. No. 6,772,346, EP-A-1549012 and EP-A-1280040 all disclose ‘community-based’ anti-malware systems in which a plurality of ‘local’ computers all connect via a network (which may be a LAN or the Internet, for example) to a central computer. On encountering a file that is not already known to them, the local computers send a request to the central computer for authorisation to run the file. If the file is recognised at the central computer, then the central computer can send permission for the local computer to run the file if the file is known to be safe or send a “deny” command if the file is known to be malicious. However, in each of these prior art proposals, if the file is not known at the central computer, then the whole file is sent to the central computer where it can be analysed to determine whether it should be regarded as safe or malware.

Id., [0007].

Count: The ’953 Publication also describes how the art kept track of the prevalence, or number of times a file was seen: “A similar community-based anti-malware system is disclosed in WO-A-02/33525. In this system, in the case that a local computer is seeking clearance to run a file that is not known by the central computer to be safe or malware, some limited audit information *about the prevalence of the file on other local computers* can be sent to a human system administrator associated with the local computer that is seeking permission to run the file. The human system administrator can therefore make a better informed

though still ‘manual’ decision as to whether or not the file is safe to run.” *Id.*, [0008] (emphasis added).

Similarly, “[i]n the system of US-A-2004/0073810, a metafile containing data about an attachment or other transmitted file is sent to a central computer. The data about that file is analysed to determine a likelihood of the transmitted file being malware. *A specific example given is that if the transmitted file has been transmitted via at least a certain number of servers, then it should be treated as malware.*” *Id.*, [0009] (emphasis added).

As demonstrated by the ’953 Publication, networked malware-detection systems, including databases, signatures, counts, and comparing information from unknown files to information from known files were well-known by the ’721 Patent’s priority date. EX-1003 ¶48. Indeed, U.S. Patent No. 7,392,543 (“Szor”), issued June 24, 2008, for instance, described a system in which “host computer systems 104 automatically detect malicious code” and “host computer systems also automatically generate and send extracted malicious code packets . . . to a local analysis center computer system,” including “the malicious code signature of the malicious code undertaking the attack.” EX-1008, 2:37-52. Szor also described a

method of sending “an extracted malicious code packet or malicious code signature of the malicious code undertaking the attack to a global analysis center,” for the purposes of “prevent[ing] the further spread of the malicious code globally” by “delivering signature updates” to client computers. *Id.*, 2:59-64.

The '953 Publication and Szor are examples, but not the only ones. In fact, Petitioners' U.S. Patent No. 7,966,650 (“Manring”) (EX-1010), for which they applied in 2008, describes the state of the art with regard to many of the '721 Patent's claimed innovations: tracking a count of the number of times an object is seen, *see* EX-1010, 8:14-21; observing and collecting information regarding the behavior of computer objects, *see id.*, 7:59-64, 8:21-28; updating an information database and distributing the updated information, *see id.*, 7:27-31; and storing computer-object information in databases, *see id.*, 8:61-9:1, 12:18-23.

VIII. OVERVIEW OF THE '721 PATENT

Notwithstanding this backdrop of the state of the art, the '721 Patent describes a distributed-architecture network consisting of a remote computer, threat servers (also referred to as web servers), and a central server (also referred to as the ENZO server). EX-1001, Fig. 3; 12:28-50, cl. 1.

The '721 Patent performs essentially the same functions as the '953 Publication, but using a three-tiered architecture rather than two. The claimed architecture consists of 1) client computers, which communicate with 2) web servers, which access data stored in 3) databases. This three-tiered architecture was a standard architecture at the time of the '721 Patent. See, for instance, CHRIS MCNAB, *Network Security Assessment* (2d Ed.) 161 (2008) (describing and depicting three-tiered data architecture in the context of web applications). A three-tiered design was commonly used at the time of the '721 Patent because it is easy to develop and adapt—as new technologies become available or a user wants to scale the system, individual tiers can be developed or expanded without affecting the other tiers.

According to the '721 Patent, conventional signature-based malware systems could detect known malware but could not detect new malware until “service providers in the field generate signatures that attempt to deal with these [new items of malware] and these signatures are then released as updates to their anti-malware programs.” *Id.*, 1:43-48. “Thus, users are at risk from new malware for a certain period of time which might be up to a week or even more.” *Id.*, 1:53-55. The '721 Patent recognizes that prior-art cloud-computing techniques can speed protection

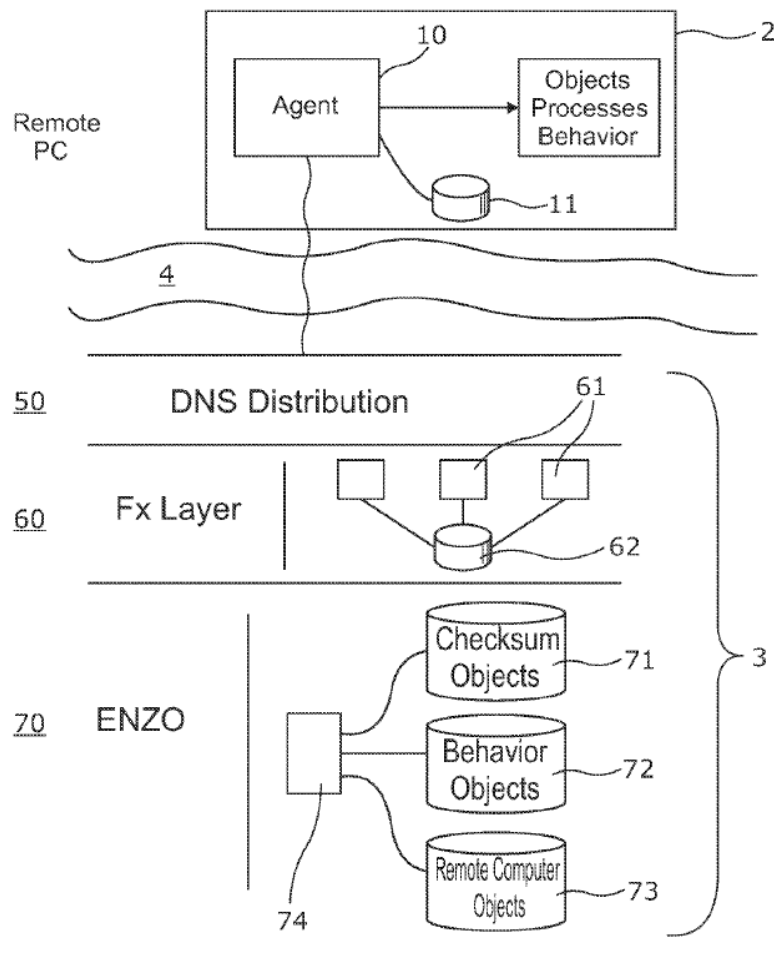
time to some extent where “protection is provided by signatures that are stored in the cloud, i.e., in a central server to which the remote computers are connected.” *Id.*, 1:58-60. However, “[t]his approach to fighting malware involves communicating, storing and managing vast amounts of data at the central server, which is a challenging problem in itself.” *Id.*, 2:29-31.

The ’721 Patent purports to provide a distributed architecture that tracks what objects are seen and how often, and updates the various distributed components as new information is learned. In particular, as shown in Figure 3 of the ’721 Patent (shown below), a remote computer can send information about a file to a web server 61 (shown in the “FX layer” in Figure 3). *Id.*, 12:28-31. Each web server 61 is connected to a database 62 “of objects that have previously been seen.” *Id.*, 33-34. The ’721 Patent describes a method of receiving, “at a base computer, . . . data about a computer object from each of plural remote computers on which the object or similar objects are stored and or processed,” a process that can “receive the data from the plural remote computers and . . . determine whether or not the object is malware and to communicate the determination to the remote computers.” EX-1001, 2:49-57. The ’721 process describes a method to “receive the data from the plural remote

computers and apply rules or heuristics against that data . . . to determine whether or not the object is malware.” *Id.*, 3:2-4.

The ’721 Patent explains that when the web server receives new information, it “checks its database 62,” *id.*, 12:36, to determine whether it has seen the information before. If it has, “the web server 61 just increases the count . . . of the number of times that data has been seen to assist in determining the popularity of a piece of software or the frequency of the occurrence of a specific event.” *Id.*, 12:38-42. Or, if the system has not seen the information before (i.e., if it “is not found in the FX database 62,” *id.*, 12:44), then “the web server requests the full data packet from the remote computer and then forwards this to the ENZO server 74,” *id.*, 12:44-46, which maintains a master record of the data from all remote computers, *id.*, 9:50-51, and “stores this data in the appropriate databases 71,72,73,” *id.*, 12:47.

The ENZO server can send this master list of all data objects “back to all of the web servers 61 in all of the geographical locations” so that “all web servers 61 are updated with information about which objects have been seen by the community.” *Id.*, 12:47-54.



Id., Fig. 3.

The Challenged Claims recite elements of a threat-data system, such as “a first remote computer,” a “first computer object,” “a first threat server,” “a first database,” “a second database,” “a database associated with a central server,” and “a second threat server.” But as further discussed below, a system using servers to distribute threat data, such as signatures, behavior information, and remote computer

*Petition for Inter Partes Review
of U.S. Patent No. 9,413,721*

information, to remote computers was well known at the time of the '721 Patent, as was keeping track of how often an object had been seen.

Indeed, during prosecution, the examiner rejected the claims over combinations involving U.S. Patent No. 8,332,946 (Boisjolie) and U.S. Patent Pub. No. 2011/0191341 (Meyer), or U.S. Patent Pub. No. 2007/0028304 (Brennan). To overcome the examiner's rejection, the applicant added the following underlined limitation in the independent claims: "providing contents of the second database to at least one database associated with a central server, wherein the contents comprise a signature of the first computer object, behavior information about the first computer object, and information about the first remote computer." The applicants argued that the prior art did not teach the added limitation.

As demonstrated below, the Challenged Claims were obvious over the prior art, including the limitation that was added just prior to allowance. This petition cites prior-art references (Liu, Tuvell, and Kester) that describe such threat-protection networks. These prior art references were not before the Examiner during the prosecution of the '721 Patent.

IX. DETAILED CHALLENGE

A. Ground 1: Claims 1, 8, 9, 14, and 15 are obvious under § 103 over Liu, Tuvell, and Kester.

Liu, Tuvell, and Kester render obvious every limitation of claims 1, 8, 9, 14, and 15.

1. Prior Art Overview

Liu was filed on September 22, 2005, and published on Apr. 6, 2006. EX-1005. Liu, therefore, qualifies as prior art under 35 U.S.C. § 102(b). Liu describes “threat protection networks,” EX-1005, [0005], in which “updated threat definition data can be distributed using a secure peer-to-peer network.” *Id.*, [0005]. It includes “at least one client computer” and “a server that stores threat definition data and is connected to the network” *Id.*, [0006]. In Liu, “clients generate threat signatures and compare them [with] threat definition data. In the event that a potential threat is unknown, a client can refer the potential threat to a server.” *Id.*, [0005]. “[T]he server compares the potential threat signature against its own copy of the threat definition data. When the server has no information concerning the nature of the potential threat, then the server can refer the potential threat to an expert system.” *Id.*, [0005] The server can update stored “threat definition data based upon determinations made by the expert system,” *id.*, [0009], and quickly

distribute the updated information to distributed client computers “via the secure peer-to-peer network,” *id.*, [0011]. The system can identify threats with a signature including a checksum generated from “the file header” or “the file body.” *Id.*, [0021]-[0023]. Thus, Liu disclosed a system to distribute threat data to remote computers, including signatures, behavior information, and information about remote computers, as well as object counts.

Tuvell was filed October 9, 2007 and published on April 10, 2008. EX-1006. Tuvell, therefore, qualifies as prior art under 35 U.S.C. § 102(b). Tuvell describes “a network management system [that] monitors malware in a mobile network.” EX-1006, Abs. As part of monitoring and identifying malware, Tuvell discloses “collection agents” that can determine whether an executable on a mobile device is malware. *Id.*, [0089]. In doing so, Tuvell discloses that the collection agent can also “notif[y] the sample collection center 1112 of the number of times it has seen the executable.” *Id.*

Kester was filed on June 1, 2005, and published on Oct. 6, 2005. EX-1007. Kester describes protecting computers from malicious software programs. *Id.*, Claim 1. Kester describes storing information identifying malicious programs

in a database associated with a computer. *Id.*, [0042]. Kester also discloses providing the contents of that database to a central database factory. *Id.*, [0054].

2. Motivation to Combine and Reasonable Expectation of Success

A POSITA would have been motivated to combine the teachings of Liu, Tuvell, and Kester for multiple reasons, including to produce the obvious, beneficial, and predictable result of facilitating the broad-scale implementation of Liu and increasing the odds of successfully identifying malware. EX-1003 ¶68.

When considering the teachings of Liu, a POSITA would also have been motivated to consider the teachings of Tuvell and Kester, since Liu, Tuvell, and Kester all pertain to the same field of endeavor of networked threat detection to identify new threats and efficiently distribute the results. EX-1003 ¶69. As stated above, Liu describes “threat protection networks” that share “threat definition data” along “a secure peer-to-peer network.” EX-1005, [0005]. Along similar lines, Tuvell describes a “network management system” that “monitors” and “analy[zes] malware,” EX-1006, Abs., and Kester discloses a system “adapt[ed] . . . over the internet” that “protects computers from malicious software programs” by “identifying” it and “determining whether the malicious software program . . . has

been previously analyzed.” EX-1007, Claim 1; *see also* EX-1003 ¶¶69. For these reasons, Liu, Tuvell, and Kester are in the same field of endeavor and are analogous to the claimed invention of the ’721 Patent.

Moreover, a POSITA would have been motivated to combine the teachings of Liu, Tuvell, and Kester to obtain predictable and beneficial results. EX-1003 ¶¶70-71. As explained above, Liu describes “threat protection networks” of “at least one client computer” and a network server that “stores threat definition data.” EX-1005, [0006]. Liu’s method compares “threat signatures” generated at the client computer to “threat definition data” and can refer an unknown threat to a server. *Id.*, [0005]. The server can update stored threat-definition data based on the determinations of the “expert system” as to whether an object is malware, *id.*, [0009], and quickly distribute the updated information to distributed client computers over the network, *id.*, [0011]. Liu suggests that a server “can provide other types of information relating to the potential threat,” *id.*, [0080], and also that the Liu server can indicate in a return code “whether the potential threat has been previously reported by another potential client,” *id.*, [0082]. Tuvell describes a system that “collect[s] data from distributed locations,” EX-1006, [0011], and can count “the number of times it has seen the executable,” *id.*, [0089]; *see id.*, Fig. 11. A POSITA

would have known to modify Liu in view of Tuvell because doing so would extend the types of information related to the potential threat, further elaborate the scale of distribution of clients within a network, produce efficiency and reliability gains, and increase the likelihood of detection of malware. EX-1003 ¶73.

Liu has “a server that stores threat definition data,” EX-1005 [0006], and explains that “updated threat definition data can be distributed using a secure peer-to-peer network,” *id.*, [0005]. A POSITA would understand that a Liu server would store the threat-definition data in a database. EX-1003 ¶97. Kester describes storing malware-related data in databases: An event may be “logged in the logging database 206,” including, for example, “the application name, time of day, and the hash associated with the application.” EX-1007, [0042]; *see also id.*, Claim 1. A POSITA would have been motivated to modify Liu and Tuvell in view of Kester because doing so would further elaborate a method of storage of Liu's threat-definition data. And since, like Liu, both Tuvell and Kester relate to networked malware detection, and Kester describes a method for storing the results of a malware-detection process, a POSITA would have been motivated to consult Tuvell and Kester in implementing the teachings of Liu. EX-1003 ¶74.

Accordingly, it would have been obvious to a POSITA to use counting and distribution (as Tuvell teaches) and database storage (as Kester teaches) when implementing Liu's malware-protection system, at least because the combination of Tuvell and Kester would facilitate the implementation, and increase the odds of success, of Liu's malware-detection system. EX-1003 ¶75.

3. Analysis

a) Independent Claim 1

[1P]: A method of classifying a computer object as malware, the method comprising:

To the extent the preamble is a limitation of the claim, Liu teaches [1P]. EX-1003 ¶82. With respect to the claimed "computer object," the '721 Patent states that "[t]he term 'malware' is used herein to refer generally to any executable computer file or, more generally 'object', that is or contains malicious code, and thus includes viruses, Trojans, worms, spyware, adware, etc. and the like." EX-1001, 1:33-36. Similarly, Liu discloses "threats," which it explains include "computer virus[es]," "spam," "spyware," "adware," "stealware," "hijacking," and "automated hacking." EX-1005, [0003], [0065]. For example, Liu explains that "Computer viruses are programs that typically seek to . . . modify and/or damage the lost

computer system,” EX-1005, [0003], and that there may be “check sums generated using a file associated with the potential threat.” *Id.*, [0008].

Liu further discloses the claimed “classifying a computer object as malware.” EX-1003 ¶83. For example, Liu discloses generating a “threat score” and using the threat score to determine “whether the potential threat is an actual threat.” EX-1005, [0091] (“The threat score can also enable a determination (148) of whether a potential threat is in fact safe.”); *id.*, [0093] (“[i]n many embodiments, a determination that a previously unknown potential threat is an actual threat is indicated by a threat score exceeding a predetermined threshold. In addition, a determination that the potential threat is safe is indicated by a threat score below a second threshold.”); *id.*, [0094] (“an expert system that classifies potential threats automatically using a threat score”). EX-1003 ¶83.

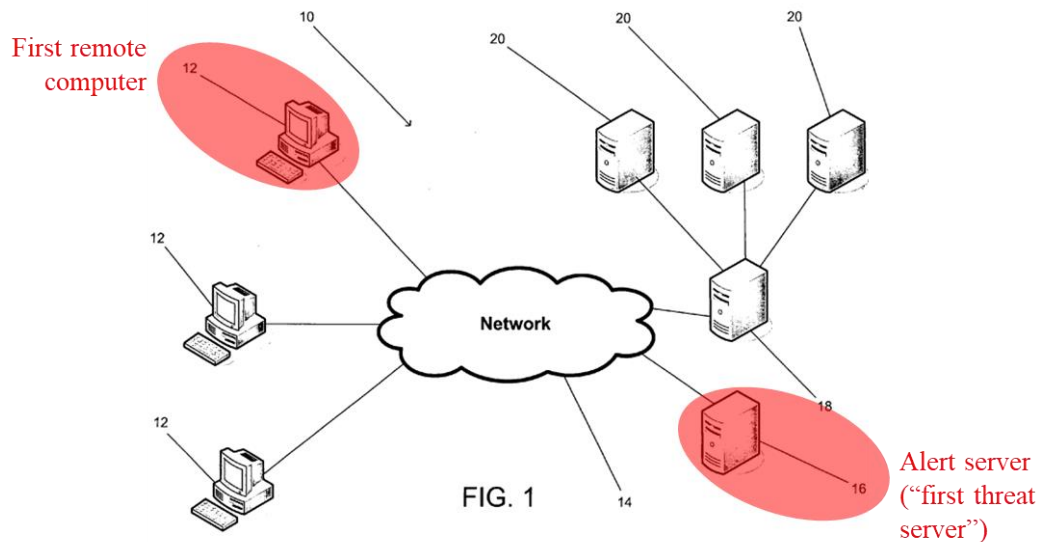
[1A]: receiving, at a first threat server, details of a first computer object from a first remote computer, wherein the details of the first computer object include data uniquely identifying the first computer object;

Liu discloses [1A]. EX-1003 ¶84.

The ’721 Patent states that “[p]lural local or ‘remote’ computers 2 are connected via the Internet 1 to a ‘central’ or ‘base’ computer 3,” and that remote computers may be “a personal computer, a server of any type, a PDA, mobile phone,

an interactive television, or any other device capable of loading and operating computer objects” where “[a]n object in this sense may be a computer file, part of a file or a sub-program, macro, web page, or any other piece of code to be operated by or on the computer, or any other event whether executed, emulated, simulated or interpreted.” EX-1001, 3:63-4:5.

“first remote computer”: Liu discloses that “[e]mbodiments of threat protection network ... use expert systems to determine the nature of potential threats to a *remote computer*.” EX-1005, Abs. Liu also explains that “Networks such as the Internet can enable rapid communication of information between computers. Unfortunately, the capability of computers to communicate is often used to victimize computer systems and/or their users.” EX-1005, [0003]. In Liu’s Fig. 1 (reproduced and annotated below), the Liu computer 12 is an example of the claimed “first remote computer”. EX-1003 ¶86.



A POSITA would understand that Liu's computer 12 is any computer that communicates over the Internet and is potentially vulnerable to threats, which is how the '721 Patent describes the remote computer. EX-1003 ¶87. For example, Liu discloses that "[c]lient software is installed on each of the computers 12 and, during operation, the computers execute the client software as a background process." EX-1005, [0067]. Liu further explains that the client software can include plug-ins for web browsers and email programs. *Id.* A POSITA would understand that Liu's computer, therefore, could be at least any computer with a web browser or email programs, such as a personal computer, PDA, or mobile phone, and is the claimed "first remote computer." EX-1003 ¶87.

“first threat server”: The ’721 Patent states that a “threat server” can be “any type of suitable server.” EX-1001, 9:19-20. Liu discloses an alert server 16 (which is an example of the claimed “first threat server”). EX-1005, [0066]. Liu further discloses that “the functions of the alert server can be performed by one or more servers.” EX-1005, [0101]. A POSITA would have known that Liu’s alert server could be composed of any server(s) and is the claimed “first threat server.” EX-1003 ¶88.

“receiving, at a first threat server, details of a first computer object from a first remote computer”: Liu teaches receiving at the alert server, details of a potential threat from computer 12. Liu discloses that “[w]hen the client software [on computer 12] encounters an unknown potential threat, the client can contact the alert server 16 for information concerning the potential threat. In the event that no information is known about the potential threat, then the client can refer the potential threat to the alert server 16.” EX-1005, [0067]; *see also id.*, [0068] (“The alert server 16 can possess information concerning the nature of a potential threat and provide the information concerning the nature of the threat directly to the computer 12 that referred the potential threat to the alert server.”).

Liu further explains that contacting the alert server for information about the potential threat includes sending a signature of the potential threat to the alert server. EX-1005, [0080] (“The process 80 commences with the determination (82) of a potential threat. The *signature of the potential threat is sent (84) to an alert server* in order to obtain additional information about the threat”) (emphasis added); see also *id.*, Fig. 4. Liu’s signature of the potential threat is an example of the claimed “details of a first computer object.” EX-1003 ¶90; see also EX-1005, [0083] (“The process 110 commences with the receipt (112) of a threat signature of a potential threat from a client.”). Thus, a POSITA would understand that Liu discloses “receiving, at a first threat server, details of a first computer object from a first remote computer.” EX-1003 ¶90.

“wherein the details of the first computer object include data uniquely identifying the first computer object”: Liu explains that “threat signatures are used to identify threats,” and that “[a] threat signature is a characteristic of a threat that is unique and, therefore, distinguishes the threat from other potentially benign files or computer programs.” EX-1005, [0004]; see also *id.*, [0072]. Thus, a POSITA would have understood that Liu’s uniquely identifying “signature” of a potential threat—which is received by the alert server from the client computer—is

the ‘data uniquely identifying the first computer object’ claimed by ’721. EX-1003 ¶91.

[1B]: determining, by the first threat server, whether the first computer object has been previously seen by comparing the data uniquely identifying the first computer object to a plurality of data uniquely identifying plural computer objects in a first database associated with the first threat server;

Liu discloses [1B]. EX-1003 ¶92.

“determining, by the first threat server, whether the first computer object has been previously seen”: In Liu, the alert server “compares (114) the threat signature to the threat definition data.” EX-1005, [0083]. As Liu discloses, there are three potential outcomes when the alert server makes this comparison: (1) if the threat signature is listed in the threat definition data, then the server sends a return code indicating the nature of the potential threat, *id.*; (2) if the threat signature is not listed, then a determination is made as to whether another client has contacted the alert server. If another claim has previously reported the threat signature, then a return code indicating that the potential threat has been previously reported and that its nature is not yet known can be sent, *id.*, [0084]; (3) if the server has not received any previous reports relating to the threat signature, then a return code can be sent that includes a request for a copy of the potential threat, *id.*, [0085] (“In the event

that the server has not received any previous reports relating to the threat signature, the server can send (122) a return code that includes a request for a copy of the potential threat.”); *see also id.*, [0005] (“In the event that a potential threat is unknown, a client can refer the potential threat to a server. In several embodiments, the server compares the potential threat signature against its own copy of the threat definition data.”). Because Liu’s alert server performs a comparison which has different results based on whether the threat signature has been seen before, a POSITA would have understood that Liu’s comparison is the claimed “determining, by the first threat server, whether the first computer object has been previously.” EX-1003 ¶93.

“by comparing the data uniquely identifying the first computer object to a plurality of data uniquely identifying plural computer objects in a first database associated with the first threat server”: As described in the preceding paragraphs of [1B], Liu describes comparing its threat signature to the threat definition. As described in [1A], the threat signature is the claimed “data uniquely identifying the first computer object.”

Liu discloses “a server that stores threat definition data.” EX-1005, Abs. And Liu discloses that threat-definition data includes threat signatures of other potential

threats. EX-1005, [0083] (“The server compares (114) the threat signature to the threat definition data. If the threat signature is listed in the threat definition data (the threat signature may be indicated as safe or as a threat), then the server sends (116) a return code that indicates the nature of the potential threat.”). Thus, Liu’s threat-definition data is the claimed “plurality of data uniquely identifying plural computer objects in a first database associated with the first threat server.” EX-1003 ¶96.

To the extent Liu does not explicitly disclose that the threat definition data is stored in a database, a POSITA would have understood that the threat definition data stored on the server would be or involve a database. EX-1003 ¶97. Liu describes that the threat definition data is searchable, *e.g.*, EX-1005, [0083] (describing determining if a threat signature exists in the threat definition data), and updateable, *e.g.*, EX-1005, [0086] (describing updating threat definition data by taking the previous version of the threat definition data and adding information to it). A POSITA would have understood that searching and inserting information are traditional characteristics of databases. Indeed, databases were well-known methods of storing of information at the time of the ’721 Patent’s invention. EX-1003 ¶98. The ’721 Patent itself assumes that the reader already knows how to implement a suitable database and does not attempt to describe database implementation.

EX-1003 ¶99. Thus, a POSITA would have understood that the stored threat definition data would be stored in a database, which is the claimed “plurality of data uniquely identifying plural computer objects in a first database.” *Id.* At a minimum, it would have been obvious to store such searchable data in a first database. *Id.*

Liu also teaches that the database that stores the threat definition data is associated with the alert server. EX-1005, [0006] (“One embodiment of the invention includes at least one client computer connected to a network, a server that stores threat definition data and is connected to the network, an expert system in communication with the server.”); *id.*, [0025] (“In a further additional embodiment again, threat definition data stored on the server, a list stored on the server and verification information stored on the server.”). Thus, Liu teaches the claimed “first database associated with the first threat server.” EX-1003 ¶100.

In any case, to the extent that Liu does not disclose that the threat-definition data is stored in a database, Kester discloses and renders obvious storing threat-definition data in a database. EX-1003 ¶101. Kester discloses that “If the requested application is found in the hash/policy table 204, the event is logged in the logging database 206. Information that is logged in the logging database 206 can include, for example, the application name, time of day, and the hash associated with the

application. The logging database 206 can also include additional data associated with the application requested. For example, a request frequency or a time of execution for the application requested can be included in the logging database 206.”

EX-1007, [0042].

[1C]: receiving additional information about the first computer object from the first remote computer when the first computer object has not been previously seen;

Liu discloses [1C]. EX-1003 ¶102.

If Liu’s alert server has not seen the potential threat before, the server can request a copy of the potential threat. EX-1005, [0085] (“In the event that the server has not received any previous reports relating to the threat signature, the server can send (122) a return code that includes a request for a copy of the potential threat.”); *see supra* [1B]. A copy of the potential threat is then sent from the computer to the alert server. EX-1005, [0088] (“When a copy of the potential threat is received (124) by the server”); *see also* Fig. 5, [0082] (“In many embodiments, the copy of the potential threat is provided to the alert server, which then forwards the copy to the threat identification system.”). The copy of the threat is an example of the claimed “additional information about the first computer object.” EX-1003 ¶104. A POSITA would find that Liu’s process of requesting and then sending a copy of the

potential threat to the alert server and threat-identification system teaches the “receiving additional information about the first computer object from the first remote computer when the first computer object has not been previously seen” claimed by ’721. EX-1003 ¶104.

[1D]: storing the details of the first computer object and the received additional information about the first computer object in a second database associated with the first threat server when the first computer object has not been previously seen;

Liu discloses [1D]. EX-1003 ¶105.

“storing the details of the first computer object”: As discussed above in [1A], Liu discloses the threat signature as an example of “the details of the first computer object.” *See* [1A] *supra*. Liu discloses “storing” those details (the threat signature): In Liu, when the server receives the threat signature, “the server compares (114) the threat signature,” EX-1005, [0083]. A POSITA would have understood that receiving and comparing would necessarily involve storing the signature so that it could be compared, and thus a POSITA would have understood that Liu discloses storing the signature as “storing the details of the first computer object.” EX-1003 ¶107.

“storing . . . the received additional information about the first computer

object”: As explained above in [1C], Liu’s copy of the potential threat is an example of the claimed “received additional information about the first computer object.” Liu also discloses “storing” that information, because storing the copy of the potential threat is required for Liu’s “process . . . used by a server to respond to a request for information concerning a potential threat.” EX-1005, [0083]. Liu discloses “the server can send (122) a return code that includes a request for a copy of the potential threat,” *id.*, [0085], and when the copy is received, “the server forwards the copy to the threat identification system,” which then “generates a report . . . used by the server to create a new version of the threat definition data.” *Id.*, [0086]. A POSITA would have understood that this process of receiving and forwarding would necessarily involve storing the copy of the potential threat, and therefore a POSITA would have understood that Liu discloses “storing . . . the received additional information about the first computer object.” EX-1003 ¶108.

“storing . . . in a second database associated with the first threat server”:

Liu teaches a second database associated with the first threat server. In Liu, “the server forwards the copy to the threat identification system,” which “generates a report concerning the potential threat.” EX-1005, [0086]. That report is then sent

to the alert server, which “create[s] a new version of the threat definition data.” EX-1005, [0086].

A POSITA would have understood that for Liu’s process to know which potential threat’s signature is associated with the report produced by the threat-identification system, Liu’s system must have a way to associate the signature with the report. EX-1003 ¶111. A POSITA would have understood that Liu’s system would associate the signature of the threat and the copy of the potential threat using a database, which was a well-known method of storing and connecting information—a POSITA would have known that storage in a database would have been a reliable design choice. EX-1003 ¶110, 112. A POSITA would have understood that the signature and copy of the yet-to-be-classified threat could be stored in a different (second) database from the already-classified threat-definition data “indicated as safe or as a threat.” EX-1005, [0083]; EX-1003 ¶110, 112.

To the extent that Liu does not disclose storing yet-to-be-classified data in a second database, Kester discloses it. EX-1003 ¶113-15. Kester claims “if the malicious software program is not identified in the first database, adding an identifier indicative of the malicious software to a second database,” EX-1007, Claim 1. It also claims that “determining whether the malicious software program associated

with the identifier [i.e., the signature] has been previously analyzed,” and “for each identifier that was not previously analyzed, associating the identifier with a digital fingerprint” and “adding the digital fingerprint to a third database.” *Id.*, Claim 1. Kester also provides that in its method the “uncategorized application database 108,” which stores data related to yet-to-be-classified objects, “can be a *separate database* from the application inventory database 103,” EX-1007, [0049] (emphasis added). The disclosure of a *separate* database for yet-to-be-classified data is by definition the disclosure of a *second* database for yet-to-be-classified data. In fact, Kester allows for many databases, not just two—see, for instance, *id.*, Claim 9 (“if the malicious software program is not identified in the third database, adding an identifier indicative of the malicious software program to a fourth database”). A POSITA would have understood Kester’s disclosure of a second, third, and even fourth database to teach that data yet to be classified regarding an object could be stored in a different database. EX-1003 ¶115. To the extent Liu itself does not disclose storage in a second database, modifying Liu to explicitly incorporate storage in a second database would have been a known technique to yield the predictable result of dividing storage and retrieval responsibilities with regard to yet-to-be-classified data between multiple databases. EX-1003 ¶115.

“when the first computer object has not been previously seen”: As explained above in [1C], Liu discloses that the copy of the potential threat is requested and received when the computer object has not been previously seen. Liu discloses that “In the event that the server has not received any previous reports relating to the threat signature, the server can send (122) a return code that includes a request for a copy of the potential threat,” and “[w]hen a copy of the potential threat is received (124) by the server, the server forwards the copy to the threat identification system. The threat identification system generates a report concerning the potential threat, which is received (126) by the server, and the report is used by the server to create a new version of the threat definition data.” EX-1005, [0085]-[0086]. Thus, as further described in the preceding paragraphs of [1D], Liu generates a report when the alert server has not seen the computer object before. As a result, a POSITA would have understood that [1D] occurs when the computer object has not been previously seen by the alert server. EX-1003 ¶116.

[1E] providing contents of the second database to at least one database associated with a central server, wherein the contents comprise a signature of the first computer object, behavior information about the first computer object, and information about the first remote computer;

Liu, Tuvell, and Kester disclose [1E]. EX-1003 ¶117.

“wherein the contents comprise a signature of the first computer object”:

As explained above in [1D], the second database contains a signature of the potential threat. *See also* [1C] *supra* (quoting EX-1005, [0085] (“In the event that the server has not received any previous reports relating to the threat signature, the server can send (122) a return code that includes a request for a copy of the potential threat.”)).

“wherein the contents comprise . . . behavior information about the first computer object”: As explained above in [1D], the threat-identification system generates a report, and that report contains the claimed “behavior information about the first computer object”: Liu explains that the report is generated based on exposing computers to the potential threat while “the behavior of the computers is observed.” EX-1005, [0087]-[0091]; *see also id.*, Fig. 6. Moreover, a POSITA would have understood that the report would need to be connected with the threat signature so that the new version of the threat-definition data could be generated. EX-1003 ¶119-20. Thus, a POSITA would have understood that the report would be stored in the same database as the signature. *Id.* As a result, a POSITA would have understood that the report is stored in the second database. *Id.*

“wherein the contents comprise . . . information about the first remote computer”: Liu describes that “[e]xamples of suspicious events include the

execution of a new program or a change in the settings of the operating system, such as an attempt to add a new program to the start up folder of a computer running the Windows® operating system manufactured by Microsoft Corporation of Redmond, Wash.” EX-1005, [0076]. Such event information would necessarily include information about the first remote computer. EX-1003 ¶121. Liu also states that “[t]he set of suspicious events can include any type of activity that is characteristic of any type of threat.” EX-1005, [0076]. Liu also states that “the server can provide other types of information relating to the potential threat,” *id.*, [0080], and a POSITA would have known that “other types of information relating to the potential threat” would include information about the computer on which the threat is located. EX-1003 ¶121.

In addition, Tuvell teaches a “receiver component” that “receives malware data,” which “includes a reference to particular devices infected or affected by the malware,” “such as current device hardware, software and/or an identifier for the infected [] device.” EX-1006, [0025], [0035]. The Kester system also tracks the remote computers hosting a particular application at each workstation. EX-1007, [0049], [0056]; EX-1003 ¶122. A POSITA would have understood that Liu with Tuvell and Kester discloses “information about the first remote computer.”

EX-1003 ¶122. Moreover, a POSITA would have known to combine Liu with Tuvell and Kester because Liu suggests that the server can provide other types of information relating to the potential threat and a POSITA would have known that the combination would have produced the beneficial result of increased problem awareness, root-cause analysis sophistication, and remediation ability. *Id.* ¶123. A POSITA would have known that it was customary to store information about the computer on which a threat was found, because—especially in a network environment that includes multiple computers—storing details about the device on which a threat is located allows a system to manage and remedy the threat. *Id.* ¶123. Finally, in Liu, object signatures may include source information (e.g., the email address or website from which an object was sent), *id.*, [0078], which is another form of behavior, in that the object was sent. EX-1003 ¶125.

“providing contents of the second database to at least one database associated with a central server”: With regard to the central server, the ’721 Patent states: “It will be appreciated that . . . the central computer and the community database are presented for convenience as single entities. As will be apparent from the following discussion, the base computer 3 can be comprised of multiple computers and servers, etc. and the community database 7 can be made up multiple

databases and storage distributed around this central system.” EX-1001, 8:32-39. The ’721 Patent also states that “[t]he ENZO layer 70 has one or more servers 74 (referred to as “central servers” or “ENZO servers” in this disclosure) connected to one or more ‘master’ databases which aggregate all the information received from all web servers 61 from all remote computers 2.” EX-1001, 9:53-57. Thus, a POSITA would have understood the ordinary meaning of the claimed central server to be any server that has aggregated information from remote computers. EX-1003 ¶126.

Liu describes a tiered distribution of updates within a secure peer-to-peer network: “In many embodiments, the alert server 16 and the computers 12 form a secure peer-to-peer network that facilitates dissemination of the update. . . . In the event that the information is not available from a peer computer, the alert server 16 can provide the information directly to the computer 12. In several embodiments, some of the functions described above in relation to the alert server are performed by one or more update servers.” EX-1005 [0070].

In Liu, “the functions of the alert server can be performed by one or more servers” and “the threat protection network can include numerous mirrored servers.” EX-1005, [0101]. “Mirrored servers” have copies of server content, so a POSITA

would have understood that Liu’s disclosure of mirrored servers means that a mirrored server will contain information about all of the objects seen on the computers and propagate that information to other alert servers. EX-1003 ¶128. As a result, Liu discloses the “central server” because any of the disclosed mirrored alert servers (or network of alert servers) in Liu is an example of the claimed “central server.” *Id.*

A POSITA would also have found it obvious to implement the functionality of Liu’s threat-protection server or servers in a hub-and-spoke architecture, with a central server, rather than a peer-to-peer architecture. EX-1003 ¶129. A POSITA would have known that the choice to use a hub-and-spoke, peer-to-peer, or hybrid architecture would have been a matter of design choice, not functionality. *Id.* A system operator chooses a particular design for a number of practical reasons (cost, redundancy, efficiency, scalability, etc.) based on the operator’s needs, but that choice does not affect the system’s functionality. *Id.* A POSITA would have known that the functionality of Liu’s mirrored alert servers could have been implemented in a “central” server, as claimed. *Id.*

Liu also discloses “providing the contents of the second database” for the further reason that a POSITA would have understood that the mirrored server would

contain the same information that exists in the alert servers, such as the information contained in the first alert server's second database. EX-1003 ¶130-31. And a POSITA would have understood that since each alert server is mirrored, each alert server will have its own databases associated with it. *Id.* Therefore, a POSITA would have understood that the mirrored server would store information (e.g., the contents of the second database) in a database associated with it. *Id.* A POSITA thus would know that Liu discloses "providing the contents of the second database to at least one database associated with a central server." *Id.*

Finally, Kester discloses sending data from the Application Inventory Database and the Uncategorized Application Database (a second, perhaps separate, database located at the Application Server Module) for inclusion in the Master Database located at the Application Database Factory (i.e., the central server). EX-1007, [0053], [0060], [0073]. A POSITA would understand that Liu, Tuvell, and Kester disclose the claimed "providing contents of the second database to at least one database associated with a central server." EX-1003 ¶132.

[1F] increasing a count associated with a number of times that the first computer object has been seen, and providing the increased count associated

with the number of times that the first computer object has been seen to the central server; and

Liu and Tuvell disclose [1F]. EX-1003 ¶133.

“increasing a count associated with a number of times that the first computer object has been seen”: Liu states that the server can provide in a return code “whether the potential threat has previously been reported by another client.” EX-[1005], [0082]. Liu may do this by keeping a count of a number of times that a computer object has been seen, and increasing the count when a computer object has been seen; it would have been obvious to a POSITA, for instance, to use SNMP MIBs to do so. EX-1003 ¶134. To the extent that Liu does not explicitly state that a count is increased, Tuvell teaches that collection agents are distributed within a network, and that “[t]he system and method works by collecting data from distributed locations, thereby increasing the likelihood that a new malware sample [is] captured once it starts spreading.” EX-1006, [0011]. Among other things, “collection agent 1102, 202 notifies 1216 the sample collection center 1112 *of the number of times it has seen the executable*.” EX-1006, [0089]; *see id.*, Fig. 11. A POSITA would have known that notifying the collection center of the number of times the collection agent has seen the executable necessarily requires increasing a

count associated with a number of times that the first computer object has been seen. EX-1003 ¶135.

“providing the increased count associated with the number of times that the first computer object has been seen to the central server”: As demonstrated above, Tuvell discloses that the count kept by the collection agents can be provided to the sample collection center. A POSITA would have been motivated to modify Liu to incorporate Tuvell’s tracking of the number of times an object has been seen and providing that information to the central server to provide greater data in monitoring and tracking potential threats. EX-1003 ¶136.

Keeping track of the number of times a potential threat has been seen in a network was well-known parameter that was tracked in malware detection systems. EX-1003 ¶137. Indeed, Tuvell states that it is a “network management system [that] monitors malware.” EX-1006, Abs. Tuvell states that collecting information about potential malware can help with deploying preventive measures: Its method “collect[s] potential malware applications from distributed locations throughout a service provider’s mobile network 302, increasing the likelihood that new malware samples are captured once they start spreading.” EX-1006, [0093]. Similarly, Liu discloses a “threat protection network” that “determine[s] the nature of potential

threats.” EX-1005, Abs. Accordingly, modifying Liu to incorporate a count and providing that count to the central server would have been a known technique to yield the predictable result of providing more information about the number of times a potential threat has been seen in Liu’s threat-protection network. EX-1003 ¶137.

In addition, Tuvell’s teachings and the background knowledge of a POSITA further motivate modifying Liu to incorporate Tuvell. EX-1003 ¶¶138-39; MPEP § 2143(I)(G). For example, incorporating Tuvell would enable Liu’s threat protection network to offer additional information about the potential threats encountered in a network. EX-1003 ¶¶138-39. A POSITA, therefore, would have been motivated to modify Liu so that a counter is kept each time an object is seen, and that count is provided to the central server. *Id.*

Additionally, a POSITA would have had at least a reasonable expectation of successfully modifying Liu in view of Tuvell in the manner described above because Tuvell teaches different information that can be collected about potential threats or malware objects and because including such a count was common in malware-detections systems. EX-1003 ¶139.

[1G] receiving, at a second threat server, at least a portion of the contents of the at least one database associated with the central server, wherein the at least a portion of the contents of the at least one database associated with the central

server include a subset of the details of the first computer object stored in the second database.

Liu discloses [1G]. EX-1003 ¶140.

“receiving, at a second threat server”: Liu teaches that “the functions of the alert server can be performed by one or more servers.” EX-1005, [0101]. Liu also teaches that “the threat protection network can include numerous mirrored servers.” *Id.* A POSITA would have understood that the server or servers performing the functions of the claimed “central server” would mirror information to another alert server (e.g., the claimed second threat server). EX-1003 ¶141. As a result, a POSITA would have understood that Liu’s disclosure of multiple mirrored servers (all included within the threat-protection network) discloses receiving threat data at a “second threat server.” *Id.*

“receiving . . . at least a portion of the contents of the at least one database associated with the central server”: Because the information the second threat server in Liu receives is mirrored from the “numerous mirrored servers” Liu discloses, EX-1005, [0101]—*i.e.*, the “central server”—a POSITA would have understood that the mirrored information would include “at least a portion of the

contents of the at least one database associated with the central server.”

EX-1003 ¶142.

“wherein the at least a portion of the contents of the at least one database associated with the central server include a subset of the details of the first computer object stored in the second database”: As explained above in [1E], the contents of the claimed second database are provided to the central server, including “the details of the first computer object stored in the second database.” Moreover, the plain and ordinary meaning of “subset” includes none, some, or all of a set. EX-1003 ¶143. As a result, because the contents of the at least one database associated with the central server include the details of the first computer object stored in the second database, the contents necessarily include a “subset of the details.” *Id.*

b) Dependent Claim 8

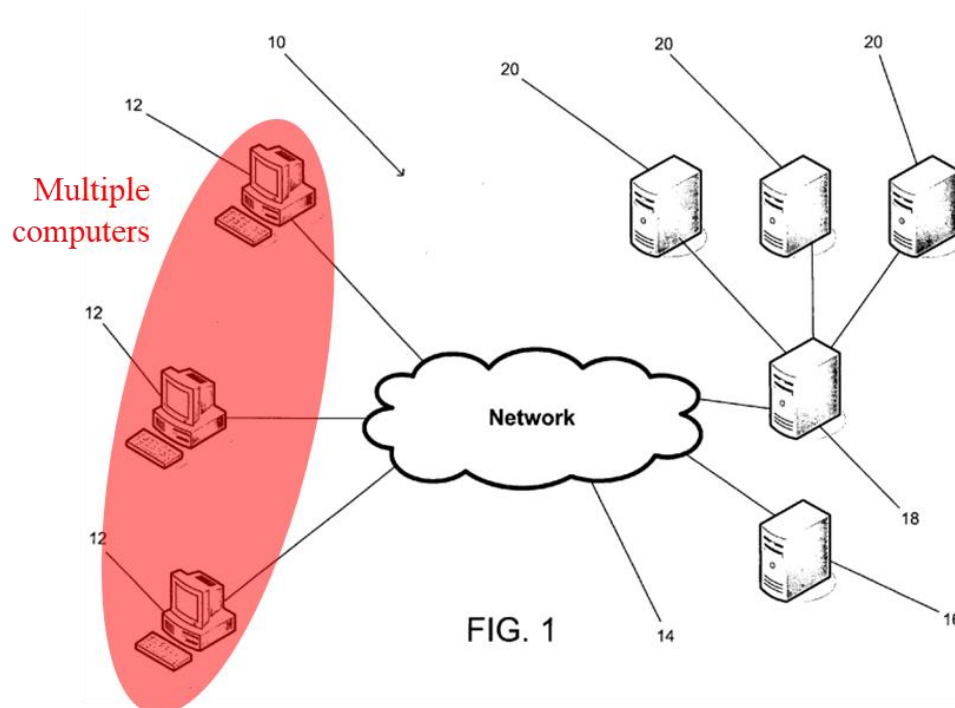
[8P]: The method according to claim 1, further comprising:

See supra Independent Claim 1.

[8A]: receiving, at the second threat server, details of a second computer object from a second remote computer, wherein the details of the second computer object include data uniquely identifying the second computer object;

Liu discloses [8A]. EX-1003 ¶145.

Claim [8A] is analogous to claim [1A] except that a second computer is sending unique details of a second computer object to a second threat server instead of a first computer sending unique details of a first computer object to a first threat server. As explained in [1G], Liu teaches that “the functions of the alert server can be performed by one or more servers.” EX-1005, [0101]; *see supra* [1G]. A POSITA would have understood that each threat server could be associated with additional computers. EX-1003 ¶146; EX-1005, Fig. 1 (showing multiple computers 12):



A POSITA would have also understood that Liu's disclosure of sending unique details of a first computer object from a first remote computer to a first threat server would apply equally to an additional remote computer connected to an additional threat server. EX-1003 ¶146. Thus, a POSITA would have understood that Liu teaches "receiving, at the second threat server, details of a second computer object from a second remote computer, wherein the details of the second computer object include data uniquely identifying the second computer object." *Id.*

[8B]: determining, by the second threat server, whether the second computer object has been previously seen by comparing the data uniquely identifying the second computer object to a plurality of data uniquely identifying plural computer objects in a third database associated with the second threat server;

Liu discloses [8B]. EX-1003 ¶147.

Claim [8B] mirrors claim [1B] except that the second threat server is determining whether the computer object has been previously seen by comparing its unique information to objects in a third database associated with the second server instead of these actions happening at the first threat server. As explained in [1G], Liu teaches that multiple threat servers can exist in the network. *See supra* [1G]. A POSITA would have understood that each threat server could be associated with additional computers. EX-1003 ¶148.

A POSITA would have also understood that Liu's disclosure of determining whether an object has been previously seen would apply equally to an additional remote computer connected to an additional threat server. EX-1003 ¶149. A POSITA would have also understood that a separate threat server would have its own associated database (e.g., the claimed third database). *Id.* Thus, a POSITA would have understood that Liu teaches "determining, by the second threat server, whether the second computer object has been previously seen by comparing the data uniquely identifying the second computer object to a plurality of data uniquely identifying plural computer objects in a third database associated with the second threat server." *Id.*

[8C]: determining that the second computer object has been seen before;

Liu discloses [8C]. EX-1003 ¶150.

Liu teaches that "[t]he server compares (114) the threat signature to the threat definition data. If the threat signature is listed in the threat definition data (the threat signature may be indicated as safe or as a threat), then the server sends (116) a return code that indicates the nature of the potential threat." EX-1005, [0083]. A POSITA would have understood that "[i]f the threat signature is listed in the threat definition data," then the object has been seen before. EX-1003 ¶151. Indeed, Liu explains

that “expert systems in accordance with the present invention can be deployed without any initial threat definition data and can be deployed in closed networks running proprietary software. An expert system trained in accordance with the present invention can rapidly build appropriate threat definition data in almost any type of networked environment.” EX-1005, [0101]. A POSITA would have understood that when Liu’s threat protection system is deployed without any initial threat definition data, and that if, subsequently, the system determines that a threat signature is listed in the threat definition data, then that means the system has determined that the potential threat has been seen before. EX-1003 ¶152.

[8D]: increasing a count associated with a number of times that the second computer object has been seen and providing the increased count associated with the number of times that the second computer object has been seen to the at least one central server; and

Liu and Tuvell disclose [8D]. EX-1003 ¶153.

Claim [8D] is analogous to claim [1F] except that count is associated with second computer object. As explained in [1G], Liu teaches that multiple alert servers can exist in the network. *See supra* [1G]; EX-1003 ¶154. A POSITA would have understood that each alert server could be associated with additional computers. EX-1003 ¶154.

As explained in [1F], Liu and Tuvell disclose keeping a count. A POSITA would have also understood that Tuvell's disclosure counting the number of times an object has been seen could apply equally to all objects in the network. EX-1003 ¶155. Indeed, it would be counterproductive to have a count of only some objects in the network as that would lead to incomplete view of which objects exist in the network. *Id.* As Tuvell states, "collect[ing] potential malware applications from distributed locations throughout a . . . network" can "increase[] the likelihood that new malware samples are captured once they start spreading" and "allow[] preventative measures to be taken sooner, potentially preventing or at least reducing any damage the malware will ultimately cause." EX-1006, [0093]. If, however, that information is incomplete, then the wrong preventive measures may be taken. EX-1003 ¶155. As such, a POSITA would have understood Liu and Tuvell to disclose keeping a count of the number of times the second computer object has been seen. A POSITA would have been motivated to combine Liu and Tuvell for the reasons explained above in [1F]. *Id.*

[8E]: receiving, at the first threat server, a count associated with the number of times that the second computer object has been seen.

Liu discloses [8E]. EX-1003 ¶156.

As discussed above, Liu teaches that there could be multiple alert servers. EX-1005, [0101] (“For example, the functions of the alert server can be performed by one or more servers[.]”). Liu also teaches that “the threat protection network can include numerous mirrored servers.” *Id.* A POSITA would have understood that the central server would mirror its information to another alert server (e.g., a second threat server). EX-1003 ¶157. Additionally, a POSITA would have understood that the mirrored information would include details about the count stored at the central server. *Id.* As a result, a POSITA would have understood that Liu teaches receiving a count associated with the number of times the second computer object has been seen at the first threat server. *Id.*

c) Independent Claim 9

Claim 9 is materially identical to claim 1, except claim 9 is a system claim. Liu, Tuvell, and Kester therefore teach claim 9 for the same reasons as set forth for claim 1. EX-1003 ¶158.

[9P]: A system for classifying a computer object as malware, the system comprising:

See [1P] *supra*.

[9A]: a first threat server arranged to receive details of a computer object from a first remote computer, wherein the details of the first computer object include data uniquely identifying the first computer object,

See [1A] *supra*.

[9B]: wherein the first threat server is further arranged to receive the details of the computer object from the first remote computer and determine whether the first computer object has been previously seen by comparing the data uniquely identifying the first computer object to a plurality of data uniquely identifying plural computer objects in a first database associated with the first threat server,

See [1B] *supra*.

[9C]: wherein the first threat server is further arranged to receive additional information about the first computer object from the first remote computer when the first computer object has not been previously seen,

See [1C] *supra*.

[9D]: store the details of the first computer object and the received additional information about the first computer object in a second database associated with the first threat server when the first computer object has not been previously seen,

See [1D] *supra*.

[9E]: provide contents of the second database to at least one database associated with a central server wherein the contents comprise a signature of the first computer object, behavior information about the first computer object, and information about the first remote computer,

See [1E] *supra*.

[9F]: and increase a count associated with a number of times that the first computer object has been seen; the central server arranged to receive the increased count associated with the number of times that the first computer object has been seen; and

See [1F] *supra*.

[9G]: a second threat server arranged to receive at least a portion of the contents of the at least one database associated with the central server, wherein the at least a portion of the contents of the at least one database associated with the central server include a subset of the details of the first computer object stored in the second database.

See [1G] *supra*.

d) Dependent Claim 14

[14P]: The system according to claim 9, wherein the central server comprises:

See supra Independent Claim 9. As discussed with regard to [1E] *supra*, Liu’s mirrored alert server is the claimed “central server,” which performs the following functions.

[14A]: a) an object database storing object signatures and metadata about objects;

Liu discloses [14A]. EX-1003 ¶168.

As explained in [1E], Liu teaches “providing contents of the second database to at least one database associated with a central server wherein the contents comprise a signature of the first computer object, behavior information about the

first computer object and information about the first remote computer.” See [1E] *supra*.

It would have obvious to a POSITA to store different types of information in different databases. EX-1003 ¶170. For example, the first threat server receives information uniquely identifying the object (e.g., the object’s signature); then, if the server has not previously seen the object, it receives a copy of the object (a copy of the potential threat), and then the threat-identification system generates and sends a report about the object’s behavior. See *supra* [1A], [1C], [1D]. A POSITA would have understood that each of these things could be stored in a different database such that the object’s signature is stored in one database (e.g., an object database storing object signatures), a second database (e.g., a behavior database storing behavior information such as the threat report), and a third database (e.g., storing information about the object such as the copy of the potential threat). EX-1003 ¶170.

Moreover, it would have been obvious to a POSITA to store these different types of information in different databases. EX-1003 ¶171. A POSITA would have known that storing information of similar types and sizes, and for use in similar ways, together in different databases would increase the system’s speed and space efficiency. *Id.* For instance, it would have been obvious to store the identifying

features of objects (e.g., signatures and metadata) together in a database because storing data that is often accessed together (and apart from infrequently accessed data) is efficient. EX-1003 ¶172.

[14B]: b) a behavior database storing object behavior information; and

For the reasons stated in [14A], it would have been obvious to a POSITA to store these different types of information in different databases. EX-1003 ¶170. In particular, a POSITA would have known that because object-behavior information may be large and variable in size, and it may include multiple instances of behavior for the same objects, it would be obvious (because efficient) to store object behavior information in its own database. EX-1003 ¶173.

[14C]: c) a computer-object database storing information about what objects are present on what remote computers.

For the reasons stated in [14A], it would have been obvious to a POSITA to store these different types of information in different databases. EX-1003 ¶¶174-75. In particular, a POSITA would have known that because information about which objects are present on which computers is critical to remediation (because object location is central to root-cause analysis and to determining where to target remediation resources), it would be obvious (because efficient) to store object location information in its own database. EX-1003 ¶175.

e) Dependent Claim 15

[15]: The system according to claim 14, wherein the first and second threat servers and the central server are implemented using cloud computing.

Liu discloses [15]. EX-1003 ¶177.

Liu teaches that “the computers and servers of a threat protection network . . . communicate via a network. In many embodiments, the network includes wired and/or wireless connections. In several embodiments, the network is a network of networks such as the Internet.” EX-1005, [0069]. Moreover, “the functions of the alert server can be performed by one or more servers.” *Id.*, [0101]. A POSITA would have known that “one or more servers,” accessed by Internet communication, disclose “cloud computing,” EX-1003 ¶178, and furthermore it would have been obvious to a POSITA to solve any problems related to significant data traffic or stringent service demands by using cloud computing. *Id.*

X. PTAB DISCRETION SHOULD NOT PRECLUDE INSTITUTION

A. PTAB should not exercise its discretion to deny institution under *Fintiv*.

Consistent with congressional intent and the goals of *NHK/Fintiv*, Petitioners took all possible steps to promote the Board’s efficiency and fairness objectives. Petitioners initiated this petition with diligence (less than ten months after waiver of

service, less than six months after receiving infringement contentions), filed a single, focused petition, and served a stipulation (EX-1011) whose scope is identical to the stipulation that the Board found to “mitigate[] any concerns of duplicative efforts between the district court and the Board, as well as concerns of potentially conflicting decisions.” *Sotera Wireless, Inc. v. Masimo Corp.*, IPR2020-01019, Paper 12 at 19 (Dec. 1, 2020) (precedential). These facts, along with the merits of Ground 1, strongly favor institution. *Sand Revolution II, LLC v. Continental Intermodal Grp.*, IPR2019-01393, Paper 24 (June 16, 2020).

1. Factor 1: Whether Institution Will Increase the Likelihood of a Stay in the District Court

Institution will enable the Board to resolve the issue of validity, and a finding of invalidity will relieve the District Court of the need to thereafter continue with the companion litigation. The District Court has made clear in prior cases that a motion to stay prior to institution of an IPR would be premature, so Petitioners have not yet requested a stay. It is unclear how the District Court would rule on a motion to stay after institution. Indeed, the Board recently “decline[d] to speculate on the likelihood of Judge Albright entering a stay after institution” and thus found Factor 1 neutral. *Western Digital Corp. v. Kuster*, IPR2020-01391, Paper 10 at 9 (Feb. 16,

2021); *see also Volkswagen Grp. of Am., Inc. v. Arigna Tech. Ltd.*, IPR2021-01321, Paper 10 at 7 (Feb. 15, 2022) (declining to speculate about the likelihood of a stay); *VMware Inc. v. Intellectual Ventures II LLC*, IPR2020-00859, Paper 13 at 12 (Nov. 5, 2020) (informative); *Apple Inc. v. Fintiv, Inc.*, IPR 2020-00019, Paper 15 at 12 (May 13, 2020) (declining to speculate regarding stay motions). Thus, this factor is at worst neutral.

2. Factor 2: District Court Schedule

The District Court schedule weighs in favor of institution. Pursuant to the District Court’s amended scheduling order on December 27, 2022 (Dkt. No. 142), the trial in this case will not begin until August 19, 2024. Based on an 18-month IPR schedule, a Final Written Decision (“FWD”) arising from this petition would issue around July 2024. Therefore, even if the trial began exactly as currently projected, the FWD would still be likely to issue before the trial even began.

Even if it were not the case that a FWD would be likely to issue before trial began, uncertainty about the trial date and the high likelihood of further delay weigh against discretionary denial. In general, District Court patent-validity litigation schedules are uncertain. Indeed, the Board has held that this factor was “neutral” even in cases where the projected trial date was close to the Board’s statutory final-

*Petition for Inter Partes Review
of U.S. Patent No. 9,413,721*

decision deadline because it has recognized that projected trial dates are uncertain, especially when projected in the early stages of litigation. In *Cizion, LLC v. Kerr Machine Co.*, for instance, the District Court trial was set “three months prior to [the Board’s] (anticipated) deadline for a final written decision.” PGR2020-00065, Paper 10 at 26 (Dec. 3, 2020). The Board explained that “[a]lthough the current schedule [in *Cizion*] indicates that trial will commence a few months prior to the statutory due date to issue a final written decision in this proceeding, evidence in the record cited by the Petitioner does indicate that the actual trial date is uncertain.” *Id.*

The *Cizion* Board credited the Petitioner’s evidence that “in the Western District of Texas, 70% of trial dates have slipped following PTAB discretionary denials.” *Id.* The Board further noted that the evidence included “multiple proceedings with trial dates close to the” same trial date. *Id.*; *see also Micron Tech., Inc. v. Godo Kaisha IP Bridge 1*, IPR2020-01008, Paper 10 at 14 (Dec. 7, 2020) (“Accordingly, even if we consider the Texas court to have set a formal trial date for a few months before the final written decision, due to the uncertainty as to this trial date, this factor is, at most, neutral to whether we should exercise our discretion to deny the Petition.”). As in *NHK*, District Court trial dates often shift. *Mylan Pharm. Inc. v. Sanofi-Aventis Deutschland GMBH*, IPR2018-01680, Paper 22, 17 (Apr. 3,

2019). The Western District of Texas is one of the country’s busiest patent courts, and trial-date shifting is likely. The general uncertainty of District Court patent-validity actions, and the high likelihood that the litigation will extend beyond its projections, weighs in favor of institution as well.

Finally, trial may be pushed even further back because this case is especially complex—Patent Owner originally asserted nine patents against five defendants, including the ’721 Patent. Those cases were consolidated for pretrial purposes. *Webroot, Inc., et al. v. AO Kaspersky Lab*, No. 6:22-cv-00243-ADA-DTG (W.D. Tex.) (Dkt. No. 49). Then, seven months after the original complaints were filed, Patent Owner moved to assert five more patents against Petitioner and other defendants. In granting Patent Owner’s motion to amend, the Court acknowledged that this case is “about as complicated as you’re going to get with patent cases,” EX-1012, 52:7-8, and the Court said it would be “amenable to adjusting the schedule” by “granting more time to address things,” *id.*, 52:22-23. Because this multi-defendant consolidated case is exceptionally complicated, it is unlikely that the District Court will dispose of the dispute over the ’721 Patent before a FWD would issue.

In any event, recent Interim Guidance² dictates that because scheduled trial dates “are unreliable and often change,” a scheduled trial date “is not by itself a good indicator of whether the district court trial will occur before the statutory deadline for a [FWD].” *Samsung Elec.’s Co., Ltd. et al v. Staton Techniya, LLC*, IPR2022-00302, Paper 13, 10 (PTAB July 11, 2022).

Thus this factor weighs strongly against discretionary denial.

**3. Factor 3: Petitioners’ Investment in the IPR Outweighs
Forced Investment in Litigation to Date**

Petitioners’ substantial investment in these IPR proceedings should counterbalance—if not outweigh—the resources invested in the co-pending litigation. It would be unjust to consider resources expended in the District Court (equally by both parties), without considering Petitioners’ resources expended to prepare this IPR petition that would be irretrievably lost without consideration on the merits, in addition to the extensive expenses that may be foregone through institution of this petition and that will otherwise certainly follow in co-pending litigation for which significant milestones exist. *See, e.g., Apple v. Seven Networks*,

² https://www.uspto.gov/sites/default/files/documents/interim_proc_discretionary_denials_aia_parallel_district_court_litigation_memo_20220621_.pdf

IPR2020-00255, Paper 13 at 12-15 (July 28, 2020) (declining to exercise discretionary denial on petitions filed nine months after the commencement of co-pending litigation where a large number of patents were included in the litigation, and a large number of claims from each patent were challenged in the petitions).

In *Sand Revolution*, even after invalidity contentions and the *Markman* hearing, the Board found that this factor weighed “only marginally, if at all, in favor of exercising discretion.” *Sand Revolution*, IPR2019-01393, Paper 24 at 11. Given Petitioners’ diligence and significant investment in filing this petition, especially this early in the litigation, this factor should weigh against a discretionary denial.

4. Factor 4: The Petition Raises Unique Issues

Factor 4 strongly supports institution. Consistent with *Fintiv*, Petitioners ask the Board to consider the unique challenges raised in the petition. Petitioners have stipulated that, if the Board institutes the present petition, Petitioners will not assert that the challenged claims are invalid on the instituted grounds in the related litigation. EX-1011. This stipulation is similar to the stipulation in *Sand Revolution* and therefore this factor strongly supports institution. *Sand Revolution*, Paper 24 at 11.

5. Factor 5: Institution Will Provide the Board an Opportunity to Invalidate Claims That Could Be Later Reasserted against Others

In the District Court litigation, as noted above, Patent Owner has asserted 15 patents against five defendants. Of those 15 patents, three are asserted against all five defendants; four are asserted against four defendants; and the average patent is asserted against 2.9 defendants. (In fact, Patent Owners asserted the '721 Patent against another co-defendant. See *Webroot, Inc. et al. v. Forcepoint LLC*, Case No. 6:22-CV-00342 (W.D. Tex.)). In other words, Patent Owner has a demonstrated history of asserting claims against multiple defendants, and the Board has an opportunity to invalidate some of those claims here. Factor 5 weighs in favor of institution.

6. Factor 6: Other Circumstances Support Institution

As explained above, the merits of the unpatentability grounds are particularly strong, weighing in favor of institution. See *Fintiv* at 14-15. And the effect on “the economy [and] the integrity of the patent system” further supports institution. *PTAB Consolidated Trial Practice Guide* 59 (Nov. 2019). The claims of the '721 Patent are very broad and purport to cover receiving, determining, and storing information about potential malware, which was already disclosed several years prior to even

the earliest priority date of the patent. The Board should consider and invalidate the claims such that they may not be asserted against other entities in the future.

B. PTAB should not exercise its discretion to deny institution under Becton and Advanced Bionics.

Furthermore, institution should not be denied under the framework set forth in *Becton, Dickinson & Co. v. B. Braun Melsungen AG*, IPR2017-01586, Paper 8 (Dec. 15, 2017) (precedential as to § III.C.5, first paragraph) and *Advanced Bionics LLC v. MED-EL Elektromedizinische Gerate GmbH*, IPR2019-01469, Paper 6 (PTAB Feb. 13, 2020) (precedential). Neither Liu, Tuvell, nor Kester was before the Examiner during prosecution. Therefore, the arguments presented in this Petition are not the same as, or substantially similar to, arguments previously presented to the Office. Thus, the first prong of the *Advanced Bionics* framework is not met. And because the first prong is not met, there is no need to reach the second prong to resolve against discretionary denial under Section 325(d)—though in any event, there are no pending proceedings before the PTAB concerning the '721 Patent, so the second prong is not met either. *Oticon Medical AB v. Cochlear Ltd.*, IPR2019-00975 Paper 15, 20 (PTAB Oct. 16, 2019) (precedential).

XI. CONCLUSION

Petitioners respectfully request that this petition be granted, that *inter partes* review be instituted, and that the Challenged Claims be found unpatentable and cancelled.

DATED: January 20, 2023

Respectfully Submitted,

By: /s/ Ryan Iwahashi

Ryan Iwahashi

(Reg. No. 63,378)

Gibson, Dunn & Crutcher LLP

1881 Page Mill Road

Palo Alto, CA 94304-1211

Tel: (650) 849-5367

RIwahashi@gibsondunn.com

XII. CERTIFICATE OF WORD COUNT

Pursuant to 37 C.F.R. § 42.24, the undersigned attorney for the Petitioners declares that the argument section of this petition (Sections I, III-XI) has a total of 13,941 words, according to the word count tool in Microsoft Word™.

DATED: January 20, 2023

Respectfully Submitted,

By: /s/ Ryan Iwahashi

Ryan Iwahashi

(Reg. No. 63,378)

Gibson, Dunn & Crutcher LLP

1881 Page Mill Road

Palo Alto, CA 94304-1211

Tel: (650) 849-5367

RIwahashi@gibsondunn.com

CERTIFICATE OF SERVICE

The undersigned certifies service pursuant to 37 C.F.R. §§ 42.6(e) and 42.105(a), (b) on the Patent Owner via FedEx overnight mail of a copy of this Petition for *Inter Partes* Review and supporting materials at the Patent Owner at the correspondence address of record for the '721 Patent:

Assignee:

Webroot Inc.
385 Interlocken Crescent
Suite 800
Broomfield, CO 80021

Counsel of Record:

Sprinkle IP Law Group
1301 W. 25th Street, Suite 400
Austin, TX

DATED: January 20, 2023

By: /s/ Ryan Iwahashi

Ryan Iwahashi
(Reg. No. 63,378)
Gibson, Dunn & Crutcher LLP
1881 Page Mill Road
Palo Alto, CA 94304-1211
Tel: (650) 849-5367
RIwahashi@gibsondunn.com